Survivability/Vulnerability Information Analysis Center

SURVIAC Bulletin

Volume XXV • Issue 1 • 2009

SURVIAC is a U.S. Department of Defense Information Analysis Center (IAC) sponsored by the Defense Technical Information Center (DTIC).

Material Flammability in Spacecraft

By Sara McAllister and Dr. Carlos Fernandez-Pello

Fire has long been a strong concern to the aircraft survivability community. There is still much basic research and testing required and on-going. Fire is also a major concern in space. This potential for injury to humans and damage to equipment has prompted NASA to fund research at the University of California, Berkeley and other institutions to investigate how fires behave in spacecraft. Fire in an enclosed compartment, like in a spacecraft, can have serious consequences – you can't open the doors, you can't call the firefighters, the smoke and toxic gases produced by the fire cannot escape or be vented, and the fire may consume the cabin oxygen very quickly. Because of the absence of gravity, the prevention and detection of fires is more difficult. The placement of smoke detectors requires special consideration because smoke and heat do not rise without gravity. Additionally, materials do not burn the same way. For example, when a candle burns on Earth, the hot gases from the flame rise, creating air currents that feed the flame and give it its familiar shape. However, without gravity, heat doesn't rise and a candle flame becomes spherical. The controlling mechanisms of the combustion process change so that fire prevention and material flammability considerations also change.

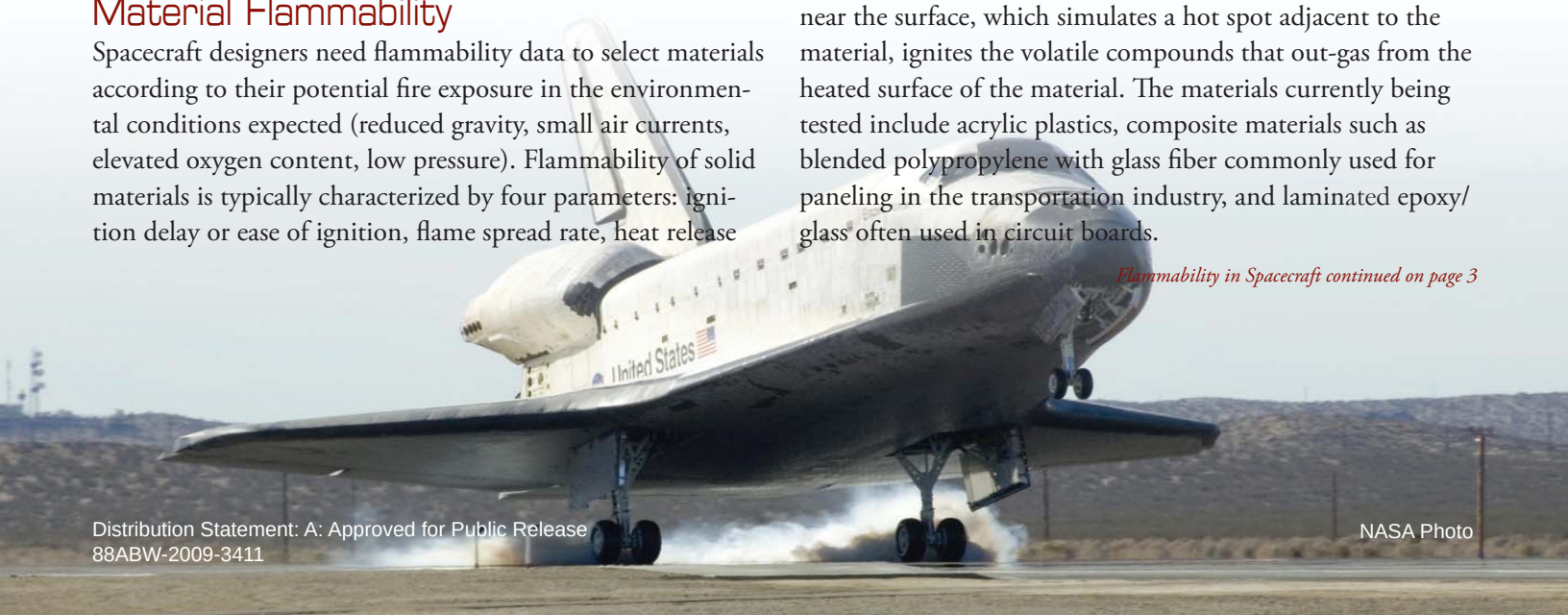
Material Flammability

Spacecraft designers need flammability data to select materials according to their potential fire exposure in the environmental conditions expected (reduced gravity, small air currents, elevated oxygen content, low pressure). Flammability of solid materials is typically characterized by four parameters: ignition delay or ease of ignition, flame spread rate, heat release rate, and toxicity. The last three parameters are important if the solid has already ignited, so it follows that there is a greater emphasis on the ease of ignition. Material flammability is primarily based on testing performed on Earth, but because of the change in the controlling mechanisms of combustion due to the absence of gravity, traditional testing methods may be inadequate. With support from NASA, researchers at the University of California, Berkeley are developing a new test apparatus, Forced Ignition and Spread Test (FIST), that will provide a more comprehensive assessment of material flammability for space applications. FIST is based on an American Society for Testing and Materials test method (ASTM E1321-93), but replaces buoyancy-driven flow with forced flow, such as the flow created by HVAC systems, to better reflect the conditions expected in space facilities.

FIST Apparatus

The FIST apparatus shown in Figure 1 consists of a small-scale wind tunnel in which samples of materials are exposed to an external radiant heat flux and varied gas flow velocities of different compositions. The external heat flux simulates a source of heat near the material and the gas flow simulates the circulation currents in the spacecraft. A hot wire placed near the surface, which simulates a hot spot adjacent to the material, ignites the volatile compounds that out-gas from the heated surface of the material. The materials currently being tested include acrylic plastics, composite materials such as blended polypropylene with glass fiber commonly used for paneling in the transportation industry, and laminated epoxy/glass often used in circuit boards.

Flammability in Spacecraft continued on page 3



NASA Photo

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
SURVIAC Bulletin: Materials Flammability in Spacecraft, Volume 25 - Issue 1	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **JAS Program Office,200 12th Street South,Crystal Gateway #4, Suite 1103,Arlington,VA,22202**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**20**	

Table of Contents

SURVIAC Bulletin
Vol XXV • Issue 1

SURVIAC, a DoD Information Analysis Center (IAC), is administratively managed by the Defense Technical Information Center (DTIC), under the DoD IAC Program. SURVIAC is sponsored by the Joint Aircraft Survivability Program (JASP) and the Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME). SURVIAC is operated by Booz Allen Hamilton Inc. The Contracting Officer's Representative (COR), can be reached at 780 TS/OL-AC/SURVIAC, Wright-Patterson AFB, OH, 45433. DSN; 785-6302, Com: (937) 255-6302 X224.

Survivability/Vulnerability Information Analysis Center

780 TS/OL-AC/SURVIAC
2700 D Street, Building 1661
Wright-Patterson AFB, OH 45433-7404

Phone: (937) 255-3828
DSN: 976-3828
Fax: (937) 255-9673

Kevin Crosthwaite
SURVIAC Director
(937) 255-3828 ext. 279
crosthwaite_kevin@bah.com

Donna Egner
SURVIAC Deputy Director
(937) 255-3828 ext. 282
egner_donna@bah.com

Steve Lawson
SURVIAC Deputy Program Mgr.
(937) 781-2139
lawson_stephen@bah.com

Gerald Bennett
Survivability Analyst
(937) 255-3828 ext. 281
bennett_gerald@bah.com

Michael Bennett
Model Analyst
(937) 781-2820
bennett_michael@bah.com

A. J. Brown
Security Specialist
(937) 255-3828 ext. 284
brown_aj@bah.com

Jim Davis
Survivability Analyst
(937) 255-3828 ext. 278
davis_jim@bah.com

Paul Jeng
Model Analyst
(937) 255-3828 ext. 273
jeng_paul@bah.com

Matt Kolleck
Survivability Analyst
(937) 781-2458
kolleck_matt@bah.com

Steve Mascarella
Live Fire Test Analyst
(937) 255-3828 ext. 288
mascarella_steve@bah.com

Jon McIntosh
Homeland Security Coordinator
(937) 781-2492
mcintosh_jon@bah.com

Linda Ryan
Publications
(937) 255-3828 ext. 208
ryan_linda@bah.com

Barry Vincent
Model Analyst
(937) 781-2456
vincent_barry@bah.com

Alfred Yee
Technical Area Task Coordinator
(937) 255-3828 ext. 274
yee_alfred@bah.com

http://iac.dtic.mil/surviac

Send us your feedback!

We would like to hear from you. Have we helped you in some way? How can we improve? Would you like to author an article for a future issue? What issues would you like to see discussed in upcoming bulletins? Modeling & Simulation? Homeland Defense/ Homeland Security? Space Survivability Issues? Unmanned Aerial Systems? Please e-mail your comments to surviac@bah.com.

Flammability in Spacecraft continued from page 1.

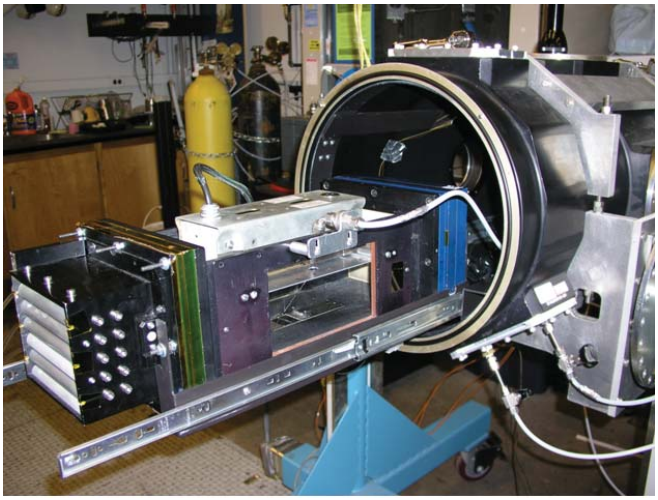


Figure 1 – FIST apparatus

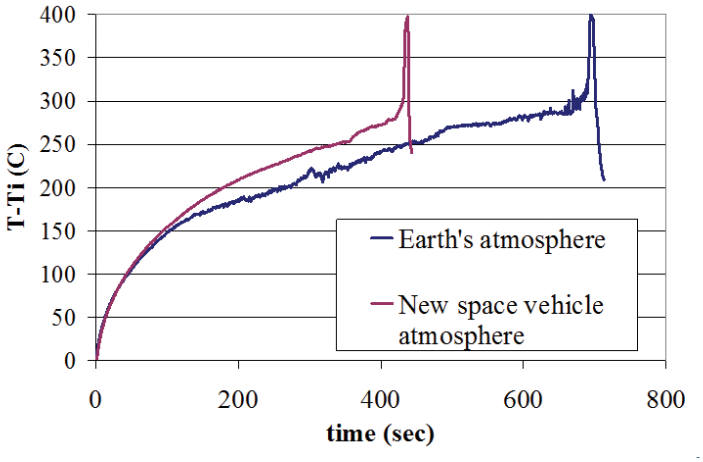


Figure 2 – Material temperature during ignition test

Current project

NASA plans to retire the Space Shuttle in 2010 and is currently designing the next generation of space vehicles. These new vehicles are being designed to operate with a different cabin environment (total cabin pressure of 52.7 to 58.6 kPa with an oxygen concentration of 30 to 34% by volume) than has been used in the past to reduce the risk of decompression sickness and the preparation time required for extra-vehicular activities (EVA). The goal of the current project is to understand just how the flammability of materials changes in this new environment.

Experiments performed to date at UCB indicate that materials ignite faster in the cabin environment proposed for the next generation of space vehicles compared to normal atmospheric conditions on Earth. Figure 2 shows the temperature of a material while it is being heated and subsequently ignited. The sharp spikes in temperature indicate when the material has ignited. From the figure, it is inferred that the material heats up faster when the pressure is reduced. In low pressure, the air is less dense and cooling by convection is less effective. In addition, it is also inferred from the figure that the material ignites at a lower temperature. Because there is less air, less fuel is needed for combustion to occur. The fuel in this case is the vapor that off-gasses from the material as it is heated. Since less fuel is required, the material doesn't have to be as hot.

Though material flammability has been a concern since the beginning of the space program, a great deal of work is still needed to understand the changes in zero-gravity environments. Of particular concern are the changes in material flammability in the proposed environment for the next generation of space vehicles. For further information on the research at UCB, please visit www.me.berkeley.edu/cpl/.

Sara McAllister, Ph.D.
University of California, Berkeley

Sara McAllister received her Ph.D. at the University of California, Berkeley in the Department of Mechanical Engineering under the guidance of Prof. Carlos Fernandez-Pello. She received her Bachelor of Science degree in Mechanical Engineering from the University of Nevada, Reno in 2004 and her Master of Science degree in Mechanical Engineering from the University of California, Berkeley in 2006. She is currently a post-doc researcher with the U.S. Forest Service at the Missoula Fire Sciences Laboratory in Missoula, Montana.

Dr. Carlos Fernandez-Pello
Professor of Mechanical Engineering and Associate Dean of the Graduate Division
University of California, Berkeley

Dr. Carlos Fernandez-Pello is Professor of the Department of Mechanical Engineering and Associate Dean of the Graduate Division at the University of California, Berkeley. He received degrees Doctor Aeronautical Engineer (1968) from the University of Madrid, Spain, and a Ph.D. in Engineering Sciences (1975) from the University of California, San Diego. He has been a visiting professor at Universities and Research Laboratories, in Japan, Italy, France, and Australia, has received various awards for teaching and research, and has been a consultant for government, and industrial, institutions in the USA, and abroad. His recent research emphasizes microgravity combustion with emphasis on material flammability in spacecraft, structural and wildland fire propagation, and micro-scale power generation using combustion.

Critical Infrastructure Protection Characterization of Threats and Targets

By Jon Wheeler, SURVIAC

Fundamental to the discussion of Critical Infrastructure Protection (CIP) is the characterization of the terrorist threat and the potential targets. From this discussion, analysts may consider methods and technologies to counter terrorist threats to our nation's infrastructure.

This article summarizes a report that surveys potential threat-target pairings for our nation's critical infrastructure and key assets.[1]

Characterization of the Threat

Without assuming limitations on the terrorist's ability to acquire the weapons inside the U.S., the threat to our nation's infrastructure must be characterized. Assuming that a terrorist could acquire any weapon needed, with the exception of some of the largest military ordnance (air-deliverable bombs and nuclear devices), an attempt was made to characterize that threat, with respect to weapons, type of person, and method of attack, as follows:

Threat—Weapons:

- Small Arms/Automatic Weapons (SA/AWs).
- Rocket propelled grenades (RPGs) and grenade launchers
- Man-portable anti-aircraft defense systems (MANPADS)
- Small explosives (hand grenades)
- Landmines
- Improvised Explosive Devices (IEDs), incendiaries, and non-lethal pyrotechnics
- Chemical/biological/small nuclear (dirty weapons)
- Hand-portable tools (saws, torches, drills, etc.) used to damage critical structure supports on bridges, etc.

Threat—Who

- Terrorists who have infiltrated into the U.S. via illegal immigration
- Terrorists recruited in the U.S. from immigrants, disgruntled citizens, or citizens who are vulnerable due to issues with debt or personal vices
- Gang leaders/members recruited by terrorist organizations
- Other criminals or revolutionaries recruited by terrorist organizations

Threats—Attack Methods:

- A terrorist can cause the US to suffer econo damage by simply accomplishing one act and then claiming they will strike again in like manner in order to cause widespread reaction and response by first-responders, law enforcement, etc. Recall the Malvo sniper incident in Washington DC.
- Avenues or access to targets may dictate form of attack.
- Actual or threatened initial attack against a target that may be designed to ambush first responders or repair personnel in a second attack to demoralize first responders.
- Attacks that are random in nature and seek to undermine one of the western world's strengths, its economic base, and/or to incite fear in the populace. Citizens' perceptions of lack of effectiveness of the civil authorities could lead to lack of confidence in government. The chaotic effects could be exacerbated by vigilantism, which in turn, could be used as a cover for further terrorist activity.
- A terrorist may decide to design an attack to achieve one of various levels of impact:
  - Functional (catastrophic target kill (infrastructure is unusable), such as dropping a complete bridge span)
  - Sufficient damage to cause temporary disruption until repaired
  - Cause service disruption due to public panic without damaging a structure
  - Cause a structure or service to injure or kill personnel or damage other infrastructure elements
  - Cause civilian authorities to draw out more resources for protection
  - Cause large numbers of emergency responses over a large period of time to over-stress governmental funding resources
  - Simply threaten to do something to incite public panic

Characterization of the Targets

The United States Critical Infrastructure is defined by the President's *National Strategy For the Physical Protection of Critical Infrastructure and Key Assets* to be "those assets, systems, and functions that we deem most 'critical' in terms of national-level public health and safety, governance, economic and national security, and public confidence." Furthermore, the nation's Key Assets are defined as "those unique facilities, such as dams, nuclear power plants, and national monuments and icons whose attacks,

1 "Critical Infrastructure Protection (CIP) Survey Using Red Team Analysis", Jon A. Wheeler. SURVIAC TR-07-040, 15 January 2007.

in a worst-case scenario, could present significant health and safety and/or public confidence consequences."[2]

The nation's critical infrastructure is categorized into eleven sectors:

- Agriculture and Food
- Water
- Public Health
- Emergency Services
- Critical Manufacturing
- Defense Industrial Base
- Telecommunications
- Energy
- Transportation
- Banking and Finance
- Chemicals and Hazardous Materials
- Postal and Shipping

Furthermore, national Key Resources and Key Assets are characterized as:

- National monuments, symbols, and icons that represent our national heritage, traditions and values, and political power.
- Facilities/structures representing national economic power and technological advancement
- Prominent commercial centers, office buildings, and sports stadiums, and other areas that provide for mass congregating for amusement, recreation, business and commerce.

Potential Target - Threat Pairings

Several potential target-threat pairings are mentioned below, with respect to selected critical infrastructure nodes.

Roads/Highways:

- Bridges and overpasses. Target bridge/overpass approaches with some sort of cratering device; target critical structural support points with cutting charges.
- Culverts and drainage pipes under roadbeds. Blocking culverts and drainage channels just downstream from critical roadways could cause flooding over the roadways.
- Roadway tunnels
- Suicide drivers in high traffic congestion
- Roads/Highways used for random standoff launches into housing/commercial areas
- Cyber attack to disrupt traffic control technology (i.e., lights, signals, etc.)
- Snipers firing at mass transit drivers

Dams/Reservoirs:

- Underwater explosives placed on the upstream side to cause damage/collapse
- Chem/Bio contamination in recreational water or potable source water
- Damage to hydroelectric generation/distribution
- Standoff launch against the structure or areas with personnel traffic, i.e.
- Cyber attack to disrupt hydroelectric generation, spillway controls, etc.
- Environmental destruction of fish and other wildlife by contamination

Light and Heavy Rail:

- Using pseudo-chemical weapons on light rail, such as simple chlorine/ammonia mixes, stink bombs, and other easily manufactured items that will cause panic and discomfort, rather than death. Subsequent threats may suggest possible escalation in order to induce public panic and law enforcement expense.
- Relatively small disruption activities, such as minor damage to rails that may go unnoticed for some time. Excavation of support materiel, diversion of storm runoff to erode support materiel, and other innocuous activities may cause derailment over some period of time if left unchecked.
- Suicide drivers versus passenger trains
- Cyber attack to disrupt traffic control

Electrical Power Production and Distribution (including nuclear and conventional plants):

- Standoff munitions/placed charges/IEDs against substations/power plants/co-gen plants
- Cutter charges (using C-4 ribbon shapes, etc) on rural high power line towers
- Simple methods for shorting across power transmission lines (chains, steel cables, etc)
- Surreptitiously rig short circuits to shock or electrocute operators/repairmen
- Cyber attack to disrupt production and distribution
- Light aircraft suicide missions against plants and/or distribution lines

Water Purification and Distribution:

- Standoff munitions/placed charges/IEDs against pump stations, manifold distribution points, control/computer rooms
- Underwater charges placed inside settling basins, clarifiers, etc., to cause them such damage as to bring them offline

2 http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

Critical Infrastructure continued on page 6

Critical Infrastructure Protection continued from page 5.

- Disrupt power to purification equipment and pumps
- Large caliber sniper fire versus computers/equipment
- Cyber attack to disrupt controls

Sanitary and Industrial Wastewater Treatment:

- Standoff munitions/placed charges/IEDs against pump stations, manifold distribution points, control/computer rooms
- Contamination of treatment chemicals
- Contamination of effluent streams
- Underwater charges placed inside settling basins, clarifiers, etc., to cause them such damage as to bring them offline
- Cyber attack to disrupt controls

Airports/Air Traffic:

- MANPADS versus aircraft ingress/egress routes
- Standoff munitions fired into airport facility
- Munitions hand-carried into airport facility, not through normal public handling areas
- Cyber attack to disrupt airport lighting, air traffic control, passenger control
- Surreptitious release of Bio/Chem weapon on passenger aircraft
- Voluntary or involuntary infected persons boarding aircraft

Port Facilities:

- Utility/Service disruption to port facilities
- Standoff munitions launched from vehicle into port facility
- Cyber attack to disrupt vehicle traffic, ship traffic control
- Small aircraft suicide attack on critical ships (i.e., liquefied natural gas carriers, etc.)
- Suicide boats versus container vessels, i.e., cargo, liquefied gas, oil tankers, etc.
- Surreptitious IED placement in berthing, channels, etc.
- Voluntary or involuntary infected persons boarding passenger vessels
- Destruction or malicious movement of buoy markers

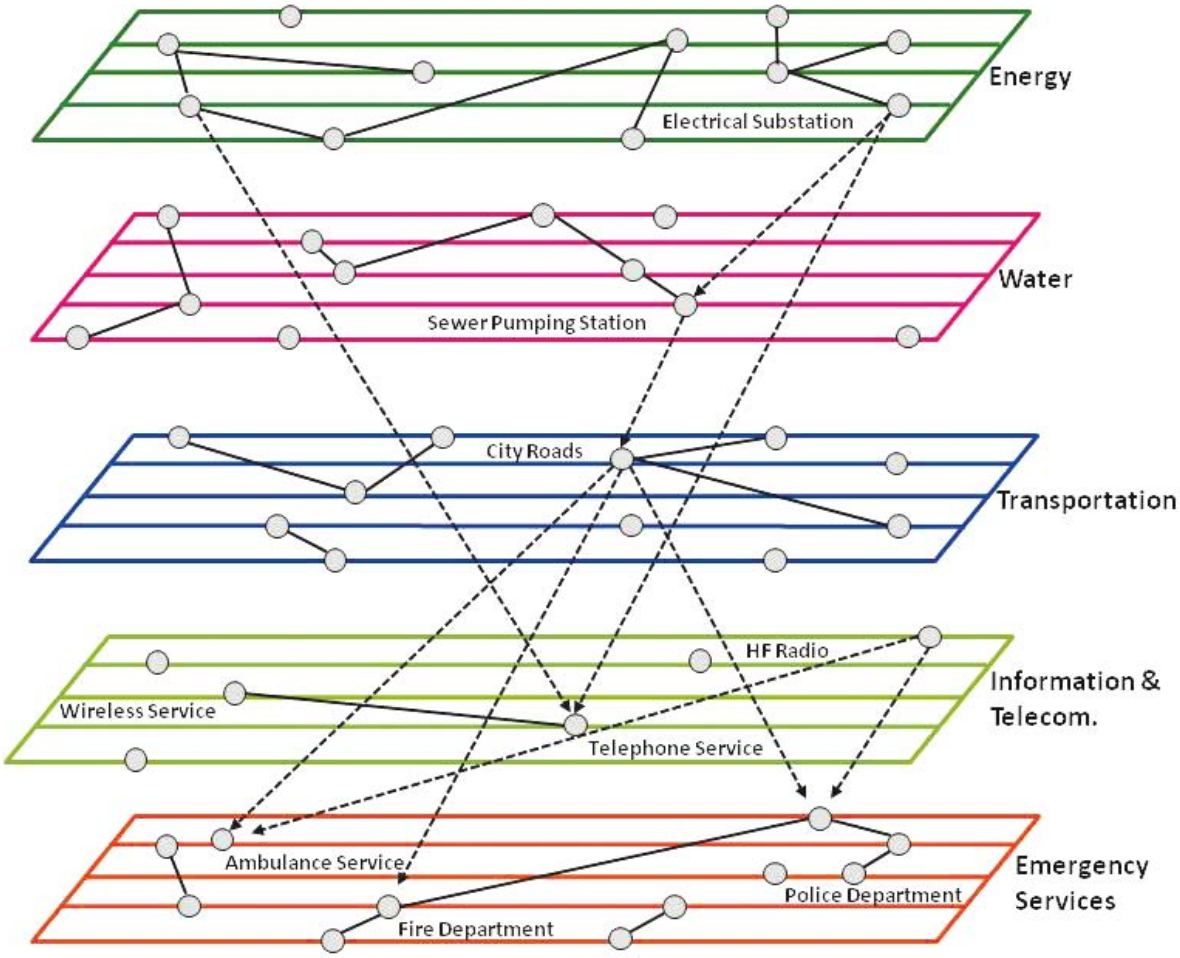


Figure 1. Compounding problem: Interdependencies between infrastructure areas.
Source: http://www.inl.gov/technicalpublications/Documents/3489532.pdf [3]

3 Pederson P., Dudenhoeffer D., Hartley S., and Permann M. (2006) "Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research", Idaho National Laboratory Critical Infrastructure Protection Division, Idaho Falls, Idaho 83415.

Cultural/Entertainment Infrastructure:

- Chem/Bio/pseudo weapons versus high density population venues, i.e., amusement parks, stadiums, theaters, etc.
- Damage to amusement park rides, utilities to disrupt services/injure people
- Standoff attack versus high density population venues
- Contamination of services (water, sanitary, food preparation and distribution)
- Disruption of emergency egress doors and routes (chain doors closed, disrupt emergency exit signage power, disrupt general lighting to induce panic)

Cultural/Historical Infrastructure:

- Launching standoff munitions with intent to damage monuments or injure/kill personnel
- IEDs randomly placed on trails/roads
- Traps built on trails for personnel injury
- Biologically infected or grievously wounded animals turned loose in park or residential areas

One of the most difficult hurdles of Critical Infrastructure Protection planning is that many of the sectors are unavoidably linked to other sectors through interdependencies, as shown in Figure 1. For example, the Energy Sector is either dependent upon or is depended on by the Oil/Gas, Transportation, Emergency Services, Water, and Communications Sectors.

Electrical substations feed the Water Sector the power to operate water and wastewater purification plants, water distribution controls, and sewage lift stations. The ability to access sanitary sewer lines are limited by traffic flow, since most city sewer lines are located underneath roadways. The electrical substation also feeds power to telephone service hubs in the communication sector. Emergency services are dependent on electrical power and communications to be able to respond to events across roadways while navigating through traffic lights. First responders from within the emergency services sector depend heavily upon wireless telephone and HF radio assets to communicate and coordinate emergency responses.

Therefore damaging or eliminating one or more nodes in one Critical Infrastructure Sector is likely to impact some portion of another sector. Likewise, first responders attending an incident targeted at one node which is part of one critical infrastructure sector may need assistance from responders responsible for one or more nodes in other critical sectors.

For more information, please contact Mr. Jon Wheeler, SURVIAC, (937) 656-3501.

Conclusion

A nation's infrastructure can become the foundation on which it can build industry, capital, and the prosperity that can lead to global power. That same infrastructure, however, can become a source of concern when an enemy might choose to damage it through acts of terrorism. To gain an understanding of how to protect the nations infrastructure, one must try to understand potential ways infrastructure can be attacked.

A terrorist attack may not be designed to destroy or even severely damage an infrastructure node, but merely to cause alarm among citizens, tie up or ambush first-responder resources, cause economic loss, or cause some response from law enforcement or citizens. This paper, generated from a Red Teaming Analysis, was intended to stimulate thinking toward potential target-threat pairings, from which law enforcement officials, government, and private sector officials can plan to prevent attack or minimize damage to infrastructure from attack.

Continuity of Operations Planning (COOP) State-of-the-Art Report

Today we are experiencing a wide range of sweeping changes in our nation's continuity policies. This State-of-the-Art Report (SOAR) is designed to help organizations in the homeland security community, particularly the Department of Defense (DoD), understand the dynamic nature of these ongoing policy changes, and how the changes will affect existing continuity plans and procedures.

This SOAR provides perspective and insight on emerging federal executive branch continuity policy—specifically Homeland Security Presidential Directive 20, National Continuity Policy; the National Continuity Policy Implementation Plan; and Federal Continuity Directives (FCD) 1 and 2—the drivers of arguably the most far reaching overhaul in Federal Government continuity guidance to occur in the last 50 years. The SOAR neither supplements nor reiterates policy—rather, it provides a broad academic overview of the fundamentals of continuity and the forces influencing their application.

This unclassified report is available through SURVIAC for Government and Contractors with current Need-to-Know. For more information please contact Mr. A.J. Brown at SURVIAC, (937) 255-3828 ext. 284, or by e-mail: alvin.brown@wpafb.af.mil

Air Force and Smithsonian Institution Work to Reduce Jet/Bird Collisions

By Marcy Heacker

Recent events, such as the emergency landing on the Hudson River by a U.S. Airways jet that had a collision with a flock of birds, have shown that birds vs airplanes is a very significant aviation issue. Marcy Heacker, a bird strike research assistant at the Smithsonian Institution, has spent many years at the Smithsonian's Feather ID Lab studying this problem. —SURVIAC

Birds vs. Planes

It can happen with no warning. Many times, the flight crew is not even aware it occurred….When a bird collides with an aircraft, the potential for a damaging event can be significant. But is this "birdstrike" issue really a problem that the aviation industry needs to address? The answer is "YES"! On average, the U.S. Air Force (USAF) loses one aircraft a year due to birdstrikes and the Federal Aviation Administration (FAA) is estimating annual losses from birdstrikes at over $500 million dollars. Birdstrikes have even been responsible for human fatalities; including the tragic incident in 1995 at Elmendorf Air Force Base where 24 people were killed when an E-3B AWACS crashed after hitting a flock of Canada Geese.

Aircraft damage from bird strike.

The USAF Bird/Wildlife Air Strike Hazard (BASH) team at the Kirtland Air Force Base Safety Center and the FAA are taking a proactive approach to understanding and preventing birdstrike events. An important part of their efforts involve an association with the Smithsonian Institution's (SI) Feather Identification Lab. The purpose of this partnership is to investigate the species of bird's causing these events. This collaboration is currently made possible by interagency agreements between the Smithsonian Institution, the USAF, and the FAA.

The SI Feather ID Lab is a highly specialized lab that processes over 3,000 cases a year for species identification from whole and fragmentary feather material recovered from birdstrikes. The majority of these cases are identified by analyzing feather fragments recovered from engines or other parts of the aircraft. The lab is housed in one of the world's largest collections of bird specimens at the National Museum of Natural History in Washington, DC. This comprehensive collection is an ideal setting for the forensic work done by researchers Carla Dove (program manager), Marcy Heacker (research assistant), and Faridah Dahlan (genetics specialist).

Bird "CSI"

While each case is different, the lab's approach to identifying birdstrike evidence depends on what kind of material is available. If there is a whole bird or partial carcass, identifications can be based on physical characters traditionally used when viewing birds in the wild - including size, color, and pattern. Wings, feathers, feet, and beaks can then be compared with the bird specimens in the SI museum collection to make a final identification. This approach is also applied when samples include only loose or fragmented feathers.

Often, there is very little material recovered from a birdstrike. Identification of samples consisting of small feather fragments, blood, and/or tissue can be examined in a couple of ways. The microscopic features of the downy part of a feather are unique for different groups of birds (ex. duck, raptor). Detailed microscopic inspection of this fluffy area of the feather can provide valuable clues to narrowing down the species identification.

The latest tool in the Feather Lab's identification toolbox is DNA analysis. Using molecular techniques to analyze minute samples of tissue and blood is an important new advancement in the lab's ability to identify bird species. After extracting, amplifying polymerase chain reaction (pcr), and sequencing the sample – the DNA sequence is compared with an online reference database of mitochondrial DNA sequences to reach a positive identification.

Many times samples are examined using more than one of these identification methods. The combination of examination results, reference comparison, and consideration of the

case details (such as date and location) leads to the most confident species identification possible.

Why Identify?

Once the lab identifies the bird species for a birdstrike case, the local airfield personnel are notified of the identification and the information is added to a comprehensive database managed by the BASH team. The application of this bird-strike data is widespread and instrumental for airfield biologists, operations managers, and flight safety personnel to focus their airfield management efforts. For example, knowing exactly which birds are active around an airfield is key to establishing efficient preventative measures and gives airfield personnel a more specific understanding to the size, behavior, and ecology of "problem" birds. Additionally, airfield personnel frequently use birdstrike identifications for establishing environmental management plans, obtaining government permits, and analyzing land-use issues.

Documenting birdstrike events with bird species identifications also provides data that can show birdstrike trends on a local or regional level. For example, a biologist could predict peaks in bird activity in certain areas, for different times of day, or different times of the year. Another good example using trends shown in birdstrike data is the United States Bird Avoidance Model (USBAM). This online prediction model uses several factors (including historic birdstrike data) to provide pilots and flight planners a reference tool for analyzing birdstrike risks throughout the United States.

Bird species identifications are also very important for aircraft designers/engineers and accident investigators. Not only can it help guide investigators to a possible cause and circumstances of an accident - if the species is known, the average mass of that bird can help interpret aircraft damage. Historic data for damaging birdstrikes was even considered when a new canopy design was developed for the F-16 jet.

Sharing the Skies

As the aviation industry grows and the use of air space increases, it can be easy to forget that there is more in the air than just planes. With the help of the SI Feather Identification Lab, the U.S. Air Force and FAA are working hard to increase the understanding, assessment, and management of this complex birdstrike issue. Ultimately, this work will continue to increase flight safety and reduce damage loss for the aviation industry - making the skies safer for both humans and birds.

Marcy Heacker is a research assistant with the Smithsonian Institution's Feather Identification Lab in Washington, DC. She received her Master's of Science and Bachelor's of Science in Biology from George Mason University in Fairfax, Virginia. She also holds an Associates Degree in Veterinary Technology from Columbus State College in Columbus, Ohio. Her work focuses on identifying bird species using whole-feather and microscopic plumulaceous feather structure. Work emphasis is on practical use of morphological and molecular feather identification methods for bird-aircraft strikes, anthropological artifacts, prey remains studies, and wildlife forensics. For more information, contact Marcy Heacker at the Smithsonian Institute HEACKERM@si.edu.

In Remembrance of BUD GILBERT

Lillard E. "Bud" Gilbert passed away on March 27, 2009 while fishing in Riverside, Ohio. Bud spent most of his childhood on Lost Creek in Greenup County, Kentucky. After graduating from high school, he attended Berea College for two years and then enlisted in the Air Force in 1951.

After returning from the Air Force, Bud married, finished college with a degree in math and physics, and taught high school math for a year. In 1960 he took a job at Wright-Patterson AFB, Ohio, where he began work as a physicist conducting research in impact physics. Mr. Dale Atkinson, who later became the chief of the Survivability Branch he organized, asked him to do some gunfire tests on an F-105 wing while Dale went to Southeast Asia (SEA) to determine the cause of aircraft losses. Based on Bud's results, Dale asked him to set up a gunfire test facility in an old gun range left over from World War II. Bud designed and supervised the building of Ranges 2 and 3 in what is now called the Aerospace Vehicle Survivability Facility (AVSF). Range 3 was a vertical firing facility to which airflow was later added to conduct realistic gunfire tests simulating aircraft in flight. Bud later volunteered to go to SEA for six months as a member of the Battle Damage Assessment and Reporting Team that was set up as a result of the recommendations from the SEA fact finding trips. He became an expert in foreign warheads and conducted a number of seminars on this subject for the Joint Technical Coordinating Group on Aircraft Survivability (JTCG/AS), now the Joint Aircraft Survivability Program (JASP.) Bud always had a number of containers of warhead fragments which greatly helped people understand warheads when he gave these seminars.

In 1986 Bud retired and continued working as a consultant in the aircraft survivability area until he retired for good in 2000 to enjoy life with his wife, children, and grandchildren. Bud was a good man and will be greatly missed by all who knew him.

Early Warning Threat Detection Using Autonomous Video Image Reconnaissance[2]

by Melvin Duran

In the current world, no facility is save from potential threats or terrorist attack, so facility security is a key issue. Facility, personnel, and asset security is built around trust in the individuals responsible for security and the reliability, capability and confidence in the technology supporting them. In most surveillance operations the objective is to obtain actionable intelligence . The most useful information is derived from constant human surveillance, which requires people dedicated to staring. However, staring for long periods is not normal. No matter how dedicated a person may be, their performance degrades rapidly in a short period [1] of time.

Advances in computer vision applied to video image reconnaissance [2] [2](VIR) technology create opportunities to meet current and new surveillance requirements that until now were not possible. Effective surveillance for large areas has not been practical in terms of expense, system complexity and operation or simply not feasible due to limitations in technology. Examples include unattended packages; airport perimeters, water reservoirs, electric power generating plants and power switching grids, oil pipelines and refineries, etc. For those that do have security, the systems are complex and have high operating costs. The Hong Kong International airport probably has the most complex security with associated high operational costs. Besides hundreds of security personnel and CCTV cameras it uses hundreds of thousands of sensors through out the airport.

Current systems are just too complex for collecting real-time actionable intelligence. Current technology focuses on post event analyses and high-speed servers that support more cameras. It still relies heavily on people staring at monitors and higher skilled personnel for its operation. Autonomous real-time CCTV video image reconnaissance is an opportunity; to reduce system complexity; dramatically enhance the security system and people performance; reduce the operating costs; and is the best opportunity to prevent rather than just record a breach of security.

Introduction

Television cameras are ubiquitous in surveillance applications. Mention video surveillance to anyone and they typically report that they already know all about it or have it. However, the nature and seriousness of threats has grown to such proportions that current surveillance capabilities are inadequate. The consequences of failure are potentially enormous and have forced a sense of vigilance higher than ever before. VIR has never been used for real-time actionable intelligence until now. More common or typical surveillance applications are; used as a deterrent to intruders simply because of the presence of cameras in a given area. Most often the video records are used to review what already happened. As current systems rely heavily on people staring at monitors, other sensors or both for detecting intrusions to an area, the probability of detecting a potential threat is low. Studies such as those conducted by the Sandia National Laboratories have shown that a person is not able to continuously watch a television monitor for more than 20 minutes before fatigue or distraction lead to their performance failure. No matter how dedicated an observer may be, it is not normal for a person to continuously stare at anything for hours. Any security system that relies on this form of surveillance has a low probability of preventing a breach in security.

Autonomous Video Image Reconnaissance

How many times its been said; 'A picture is worth a 1000 words'. When used to it's full capability, real-time CCTV video image reconnaissance can instantly produce a picture of a potentially dangerous situation for immediate assessment. This provides on-site responders actionable intelligence to quickly assess the situation and decide on an appropriate response. Early warning VIR is an excellent tool to provide real-time intelligence to on-site personnel.

VIR begins with capturing and assessing each picture from a video stream of pictures for any changes. Features such as low sensitivity, global pixel change filtering and efficient processing through the algorithms are essential components. Software intelligence should permit rapid computer analysis to assess if the change is relevant or not. This preliminary analysis eliminates human interaction from the process until a relevant change is detected.

1 Actionable intelligence is sufficient information to conduct a real-time assessment of the current situation.

2 Video Image Reconnaissance is continuous acquisition of television camera images useful for conducting a real-time assessment of the camera scene.

Video detection technology began with Video Motion Detection technology but CCTV systems were plagued with high false alarm rates for low sensitivity settings. This dramatically limited their range of usefulness with the result that most surveillance still relied on people staring at monitors and or other detection sensors.

Core Technology

Variant-iD Technology (when applied to the security application) successfully overcomes many known problems with CCTV surveillance. These include; high false alarm rates; slow speed; and limited range. Variant-iD is state-of-the-art patent pending image processing algorithms, developed by the Jemez Technology Corporation. The basic function of the algorithms is to continuously find and assess the differences between a current and previous picture of the same object or area. Following several years of development, the algorithms have evolved into commercial video surveillance applications. The end result of this effort is video image reconnaissance VIR from autonomous CCTV surveillance.

Image change detection algorithms continuously check each picture in a video stream extracting, showing and tracking all changes in the scene from a wide field-of-view camera.

The following figure is an example of change locations automatically exported to a telephoto camera. This is an example of advanced technology for hands-off surveillance to provide automatic tracking and quick assessment of an intrusion.

A fundamental requirement for operation of early warning video surveillance is simplicity. The system should not be an operational burden. On-site security personnel should have a real-time tool to aid in dealing with a potentially dangerous situation. For the operator, it should be see the situation, determine a response and respond. Using image change detection, performance of the Variant-iD technology permits this extreme autonomous video operation. Intelligent foundation software assesses the changes; updates the system for 24/7 operations; is easily adapted to changing surveillance requirements and areas; and permits access and motion where the operator allows.

Current Surveillance Systems

Jemez Technology conducted surveys of current CCTV applications in industry. Our purpose was to learn what, why and how CCTV was being used for surveillance and what the successes and failures were. There were no successes. What we found was not surprising. Current CCTV video and or other intrusion detection sensors performance simply cannot meet the demanding requirements for video detection.

In spite of having sensors and or CCTV surveillance capabilities, security and ultimately intrusion detection rely heavily on people or usually does not happen.

Studies

Chain Store

Many chain stores have serious problems with theft from their storage areas. Wal-Mart reports more than $2 billion dollars annually lost to theft. One retail food store associated with a large chain was equipped with video surveillance to watch for theft in their storage areas. We learned that all their video cameras had been turned off. They could not afford to spend the time to watch a monitor continuously nor spend the time reviewing 24-hour video recordings. Based on conversations with the store director; our conclusion is that they accept whatever the losses are simply because there is no good alternative.

State Prison

A state prison used shake detectors on the fence surrounding the perimeter of the prison to detect any attempt to climb the fence. We learned all sensors had been turned off due to high false alarms caused by wind, prisoners purposely shaking the fence and debris hitting the fence. They installed cameras to monitor the perimeter but found guards could not watch the monitors continuously. The alternative in practice is a guard continuously driving around the perimeter for actual detection of an attempted escape.

Art Galleries

Art galleries and museums are examples of high dollar value storage. Santa Fe, NM has had a series of burglaries involving high value art. The most valuable reported theft of artwork was a $500,000 painting. Each of the galleries interviewed

Early Warning Threat Detection continued on page 12

Early Warning Threat Detection continued from page 11.

reported they have security systems installed and always turned on after hours, some during open hours. While there have been several burglaries in the last 12 months, only one of the security systems detected the intrusion but did not have any useful information.

Input from Experts

Los Alamos National Laboratory

Security personnel from the laboratory spent considerable time evaluating Variant-iD Technology. Their purpose was not only to assess the image change detection technology but also to suggest operating features that would make the system more useful to the on-site security person.

Beta Site

We installed and have an outdoor single camera surveillance system using image change detection operating at the Bernalillo County Metropolitan Detention Center. The prison has operated the system 24/7 for approximately eight months. The purpose of the installation was to provide surveillance of an area 60 feet by 2000 feet in place of assigning guards to this activity. To date the system is performing to their expectations and have no operational problems.

Transition To An Actionable Intelligence Gathering System

It is extremely important to know and understand the surveillance application and requirements. Equally important is to know and understand; the user's capabilities and level of knowledge for system operation; what is useful real-time information; and their expectations for system operation. Too often, a user does not really know what may be the optimal surveillance system for their situation. In too many examples of security systems, real-time actionable intelligence comes from people.

For example, motion is only one of several factors that can be a measure for alarm. Changes in shape, lighting from dark to light and vice versa, and small changes in busy scenes can be significant indicators for security. Traffic permitted around keep out areas can be confusing and a distraction to operators, particularly in busy scenes. Many years of experience in remote sensing detection technology and information from its studies and experts were applied to produce the Variant iD. Variant iD's algorithms and operating software were integrated to permit rapid computer assessment of pictures from video streams to check for changes in the TV camera scene. This software development integrated with off-the-shelf hardware became the foundation system for true real-time video image reconnaissance. In any surveillance requirement to watch for changes where there should not be any, VIR technology can take the human out of the loop.

The priority and primary purpose of surveillance is to detect potential threats or problems as early as possible. Current systems in use today suffer from; high false alarm rates; slow speed; limited range (10s of feet); limited or unreliable detection capability; and the most serious, human error caused by fatigue and distraction. The emphasis in the CCTV industry has been toward more advanced recording capability for post event analysis. Servers are faster; support more cameras and other detection sensors all leading to more complexity, more guards and programmers, and higher operating costs. Until now the front-end sensor detection ability has not been useful. Current technology to achieve the performance necessary for long range and broad area surveillance was simply not reliable.

Cases In Point

The U.S. Border Patrol uses thousands of TV cameras and tens of thousands of motion and intrusion detection sensors buried at key locations. The sensors are used in place of relying on people staring at monitors. None of the CCTV systems use video motion detection. In spite of these efforts, hundreds to thousands of illegal aliens are able to cross the border into the US on daily basis.

The Bernalillo County Metropolitan Prison uses more than 250 cameras to monitor every door in the prisoner detention area. Each camera and doorway system is equipped with push button switches wired into the Master Control Room. Pressing a switch alerts a guard whenever anyone wishes to pass through the portal.

In these examples, computer vision in the form of VIR technology would have reduced the costs associated with installation and maintenance.

Next Generation

Variant iD focuses on detection technology that takes people out of the loop until they are needed. While it can work with other types of sensors, it does not require them. The ease of operation using VIR technology is reflected in an operating system developed as a hands-off operation including and during an alarm. Its performance ability is confirmed by more than 8 months of 24/7 outdoor operations in the Bernalillo County Metropolitan Prison. Real-time operation at the prison demonstrates a high confidence in the probability of detecting intrusions with minimal operating costs.

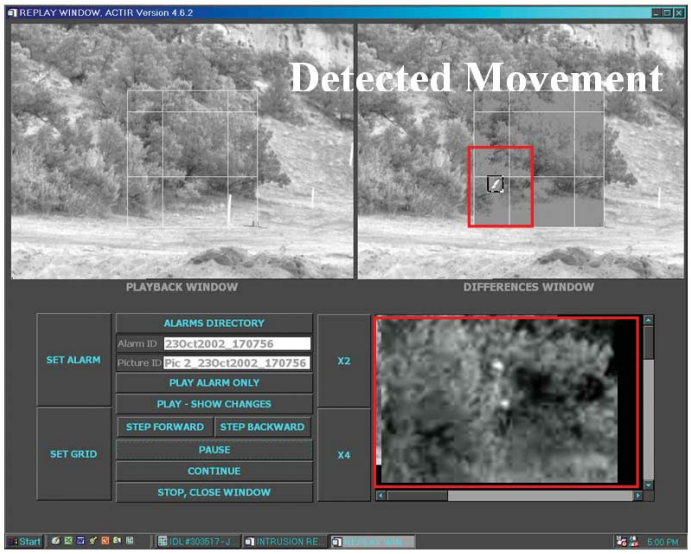
The following figure is Jemez Technology's basic VIR surveillance system. It consists of a wide field-of-view camera inside of the dome and a telephoto camera show suspended below the dome.

VIR Detector Assembly

The system is an example of off-the-shelf hardware integrated with advanced computer vision, Variant-iD technology, and software. Computer vision in the form of advanced image processing algorithms can reduce or depending on the application, eliminate hardware development.

VIR Detector Assembly

The following figure is an example of collecting actionable intelligence. The test was conducted using only a single wide field-of-view camera system with digital magnification. In this example, a person ~6 feet tall was moving behind a bush. The image change detection software was used to detect his motion before actually stepping out from behind the bush. The purpose of the test was to assess the software capability to find changes in small groups of pixels, combine them with others and assess whether or not to report a change.



This test was conducted at the Los Alamos National Laboratory's shooting range at a distance of 220 feet using a singlewide field-of-view camera. The person's arm was recoiling from just firing a handgun. The system formed an image of the person's arm while still behind the post by integrating smaller pixel groups to form the larger image.

For many applications, speed and sensitivity are important factors. During testing at the Los Alamos Laboratory, handguns and rifles were fired at distances up to 100 yards.

Gunfire is an event that typically is over in approximately 0.2 seconds. Detection of the first flame and debris exiting the barrel of handguns is shown in the following example. This demonstrates the speed of the image processing algorithms to detect small and fast occurring changes.

Conclusion

In this paper we have discussed the status of current surveillance systems and the applications and importance for advanced technology systems. We have outlined examples of studies and tests where the application of real-time video reconnaissance technology demonstrated its usefulness in producing actionable intelligence.

We believe that early detection, notification and warnings are the priorities for surveillance systems. Actionable intelligence is paramount and minimizing people having to interact with the system to collect it is extremely important. Distributing the information should also be a very high priority. Communication and information technology are far ahead of surveillance technologies. The technology to quickly and broadly distribute information is already available. Development should focus on and emphasize the front-end sensors for early warning and high performance surveillance

Early Warning Threat Detection continued on page 14

Early Warning Threat Detection continued from page 13.

applications. Computer vision in the form of image change detection technology applied to VIR provides solutions to eliminate and overcome the most significant surveillance system problems. Jemez Technology's Variant-iD technology provides an example of the capability to acquire actionable real-time intelligence in time for it to be useful.

For further information, contact Melvin Duran, Jemez Technology Corporation, 68 Canada Circle, Los Alamos, NM 87544, Telephone (505) 661-0269.

Mr. Mel Duran has more than 30 years of technical contributions for the development of advanced remote sensing instrumentation and systems. At the Los Alamos National Laboratory, he was manager of a multidiscipline engineering group consisting of more than 100 persons annually supporting more than 50 technical programs and projects. The projects were for national treaty verification programs using military satellite systems. These included satellite sensors and systems for particle, x-ray, rf and visual event detection applications.

He was the Project Engineer for a "Star Wars" program to develop a Neutral Particle Beam Accelerator and demonstrate autonomous performance in flight using an Aries rocket; Beam Experiments Aboard Rockets (BEAR). He was the startup Project Engineer for the Laboratory's first satellite, ALEXIS, Array of Low Energy X-ray Imaging Sensors. The Accelerator program was successfully completed at a cost slightly more than $100 million dollars and Alexis at slightly under $40 million.

Mark your calendar

for the

Winter Joint Model Users Meeting

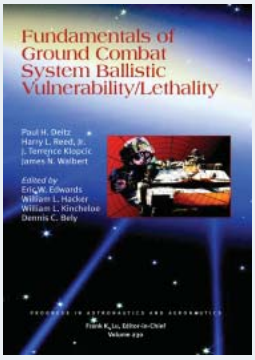
(JMUM)

17-19 November at Nellis AFB, Nevada

For more information contact Paul Jeng, SURVIAC

937-255-3828 x273 or jeng_paul @bah.com

Fundamentals of Ground Combat System Ballistic Vulnerability/Lethality



With contributions from more than 50 vulnerability/lethality (V/L) professionals in Government and industry, this 300-page text provides a comprehensive look at the basic history, terminology, processes, tools, and applications associated with the V/L discipline. It's intended to serve as both a foundational textbook for new V/L analysts, testers, developers, researchers, and scientists as well as a ready-reference for those practitioners already working in the field.

The book's major themes include:

- The history of V/L analysis
- The role of V/L in materiel design, development, and acquisition
- The V/L analysis process
- The Missions and Means Framework
- Initial representation
- Damage mechanisms
- Component dysfunction
- Personnel vulnerability
- Wound ballistics
- Target response
- Tactical utility
- Vulnerability assessment
- Measures of effectiveness
- Fault trees and degraded states
- Networked systems
- Modeling and simulation tools and methods
- Verification, validation, and accreditation
- System acquisition and life cycle issues
- Vulnerability reduction
- Tactics and doctrine.

Also included are an extensive bibliography and appendices that provide more in-depth discussions on fragment penetration, behind-armor debris characterization, PCD|H estimation, and applied VV&A processes.

For information on obtaining this book, Government employees may contact A.J. Brown, SURVIAC, (937) 255-3828 ext. 284. All others may obtain this book through AIAA, 800.682.2422, www.aiaa.org.

Insensitive Munitions - Minimizing Collateral Damage Through Development and Application of Advanced Technology

by Mr. Ken Tomasello, Naval Ordnance Safety and Security Activity and Mr. Gerald King, Booz Allen Hamilton Inc.

There have been – over the course of several decades –numerous incidents in which the collateral damage from conventional munitions resulting from accidents or combat actions has killed or injured our own Service members. These events have, fortunately, been few in number but they can have disastrous effects because of the inherent nature of explosives and propellants. The Insensitive Munitions (IM) program is a proactive approach to minimize such collateral damage from munitions exposure to unplanned stimuli while maintaining munitions performance. The programmatic requirements for IM are integral to munitions development and acquisition as indicated in Figure 1, below.

U.S. LAW

USC, Title 10, Chapter 141, Section 2389
December 2001: "2389. Ensuring safety regarding insensitive munitions. The Secretary of Defense shall ensure, to the extent practicable, that insensitive munitions under development or procurement are safe throughout development and fielding when subject to unplanned stimuli."

Department of Defense Policy

DoDD 5000.1, May 12, 2003: E1.1.23.Safety. "...All systems containing energetics shall comply with insensitive munitions criteria."

Joint Chiefs Policy

Chairman, Joint Chiefs of Staff Manual CJCSM 3170.01B, May 11, 2005: "At a minimum, these CDDs and CPDs will contain the statement, 'Munitions used in this system will be designed to resist insensitive munitions threats (unplanned stimuli)." "...IM waiver requests require approval by the JROC..."

OSD(AT&L) Policy

OSD Memorandum: 21 July 2004 "...annual IM Strategic Plans will be the vehicle to submit and consolidate IM waiver requests."

Figure 1. Insensitive Munitions Requirements Span Statutory and Regulatory Arenas

The IM requirements, promulgated in MIL-STD-2105C address potential thermal, shock, and impact threats as shown in Table 1. In strong coordination with our allies these requirements are also identified in North Atlantic Treaty Organization Standardization Agreements (NATO STANAGs).

The objective of the IM effort is to develop and deploy conventional munitions that minimize the collateral damage when threat stimuli are encountered. This can be especially significant in asymmetric warfare and when military operations are necessary in dense urban environments. The Office of the Secretary of Defense has established a Department of Defense major science and technology (S&T) program to foster the IM technology required to meet this objective. This Joint IM Technology Program (JIMTP) leverages the expertise of engineers and scientists across the Department of Defense (DoD) to pursue a total systems approach to IM.

The JIMTP is focusing on five technology gaps as shown in Figure 2. The rationale for pursuing these five technology thrusts are: (1) these munitions focus categories are based on input from weapon Program Executive Officer (PEO) and IM subject matter experts; (2) emphasis is placed on high-priority, high-payoff areas; and (3) expectation that trickle-down technology will benefit other munitions component areas. Such a focused approach maximizes the benefits achievable from the investment in technology development.

Major task areas, therefore, focus on: blast/fragmenting warheads, reduced smoke propellants, large solid rocket motor propulsion, large caliber gun propellants, and anti armor

Table 1. Insensitive Munitions Technical Requirements

IM Test	Threat	Passing Criteria	Stimulus Environment	NATO STANAG
Fast Cook-off (FCO)	Liquid Fuel Fire (e.g., truck or an aircraft on a flight deck)	Burning	Rapid heating	4240
Slow Cook-off (SCO)	Slow Heating 3.3°C/Hr (e.g., fire in adjacent magazine, store or vehicle)	Burning	Slow heating	4382
Bullet Impact (BI)	.50 Cal M2AP 3 round bursts (e.g., small arms from terrorists or combat)	Burning	Low level kinetic impact such as from small arms fire	4241
Fragment Impact (FI)	18.6 gram fragment traveling 8300 +/- 300 fps (e.g., bombs, artillery, or IEDs	Burning	Combined shock, mechanical, thermal such as artillery fragments	4496
Sympathetic Detonation (SD)	Detonation of a single donor (detonation of adjacent stores)	Explosion or less (no propagation of detonation)	Detonation of a similar item in a stack or pallet	4396
Shaped Charge Jet Impact (SCJI)	81-mm Precision shaped charge (e.g., RPG, Bomblets, ATGMs: combat or terrorists)	Explosion or less	Shaped charge weapons	4526

Insensitive Munitions continued on page 16

Insensitive Munitions continued from page 15

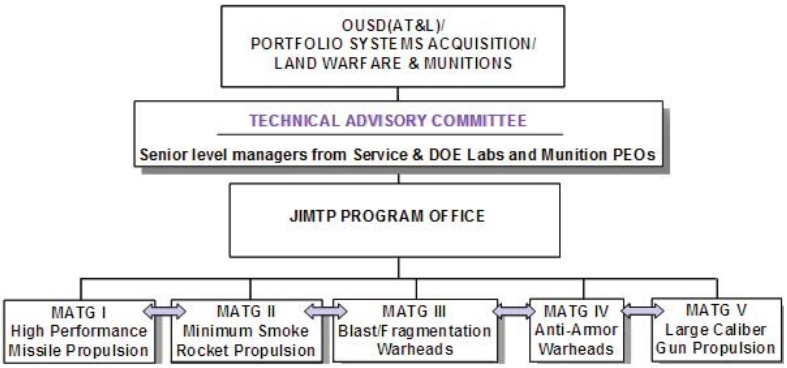


Figure 2. Joint IM Technology Program Construct

warheads. These work areas were developed from priority munitions IM technology shortfalls identified by program managers.

There have been successes in the development and integration of IM technologies. Notable among larger munitions is the AGM-158 Joint Air-to-Surface Standoff Missile (JASSM). The JASSM has achieved IM compliance, a significant accomplishment for a munition with a 1,000 pound warhead. The JASSM explosive fill is AFX-757 which is an extremely insensitive explosive developed by the Air Force Research Laboratory/High Explosives Research and Development Facility, Eglin AFB, Florida. JASSM also employs thermal venting to mitigate thermal threats.

Other significant munitions that have achieved IM compliance include the Anti-Personnel Obstacle Breaching System (APOBS); the Standoff Land Attack Missile (SLAM); and the M1028 120mm Tank Round. Additionally, more than two dozen smaller munitions families are IM.

IM compliance is a challenging technical endeavor. The benefits are maximizing forces' ability to stay on station and continue operations and maximizing force protection. IM can also minimize loss of life from our own munitions; minimize collateral damage; and minimize stockpile losses from sympathetic munitions reactions. The DoD and the Services have in place forward leaning programs to leverage previous successes and drive IM improvements throughout the conventional munitions inventory.

2009 SURVIAC Liaison Workshop

The Survivability / Vulnerability Information Analysis Center (SURVIAC) invites you to join our annual SURVIAC Liaison Workshop at our facility at Wright-Patterson AFB, Ohio on 28-30 September 2009.

SURVIAC implemented this innovative liaison program to expand the survivability/ vulnerability user base through the on site training of Government and Industry volunteers located remotely from the Wright Patterson AFB, Ohio office. The purpose of the Liaison training program is two-fold. The objective is to increase the knowledge about SURVIAC and what resources we have to support other agency's/company's mission. The second objective is to inform us about your respective needs so that we can better support you in the future. The workshop is open to government and industry personnel. Three days will be spent investigating databases and libraries, performing searches, reviewing products and models, reviewing Technical Area Tasks, becoming familiar with key survivability and lethality agencies, as well as simply becoming familiar with the day-to-day operation of the SURVIAC office. Discussions will be held relative to ongoing efforts in the survivability/lethality communities and a briefing will be presented by the Defense Technical Information Center (DTIC) Information Analysis Center (IAC) Program Office. Each participant will be informed on how the IACs and DTIC interrelate and how they are available to support the varied warfighter missions. The last day will be spent discussing the needs of each liaison and how a more effective relationship through this program might be established. In addition to the instruction, attendees will come away with the realization that a vast amount of information is available both at SURVIAC and throughout the community.

The cost of this workshop is $1000.00. For more information on this year's workshop please contact Donna Egner, (937) 255-3828 x282, e-mail egner_donna@bah.com.

Model News

At the SURVIAC Technical Coordinating Group meeting held in February 2009 three decisions were made concerning the modeling services from SURVIAC. 1)The model entry procedures are to be revised and incorporated by SURVIAC. JASP and SURVIAC are coordinating the suggested revisions to what was presented. 2) The model distribution fee of $500 for contractors will be suspended starting July 1. This will be revisited after one year to assess the effects on the SURVIAC core operations. 3) The Joint Threat Engagement and Analysis Model (JTEAM) will be archived due to the lack of a government model manager and support contractor. For further information on these or other model related topics, contact Barry Vincent at (937) 781-2456

Models Distributed by SURVIAC

The Survivability/Vulnerability Information Analysis Center (SURVIAC) is a U.S. Department of Defense Information Analysis Center (IAC) sponsored by the Defense Technical Information Center (DTIC)

Acronym	Model Name	Version No.
AIRADE	Airborne Radar Detection Model	7.4
ALARM	Advanced Low Altitude Radar Model (Includes EARCE 2.5)	5.2
BLUEMAX 5	Variable Airspeed Flight Path Generator	1.0.2
BRAWLER	Air-to-Air Combat Simulation	7.1
*BRL-CAD	Ballistic Research Laboratory Computer-Aided Design Package	7.14.8
**COVART	Computation of Vulnerable Area Tool	6.0
ESAMS	Enhanced Surface-to-Air Missile Simulation	4.0
**FASTGEN	Fast Shotline Generator	6.0
FATEPEN	Fast Air Target Encounter Penetration Program	3.0.0
IVIEW 2000	Graphical User Interface for Output Simulation	1.0E
JSEM	Joint Service Endgame Model	1
LELAWS	Low Energy Laser Weapons Simulation	3.0
RADGUNS	Radar-Directed Gun System Simulation	2.4.1

* For more information regarding BRL-CAD documentation contact Mr. Dwayne Kregel at the SURVIAC Aberdeen Satellite Office, (410) 273-7722.

** Model is part of the Vulnerability Tool Kit

For further information on how to obtain these products and how to establish need-to-know certification, please contact SURVIAC at (937) 255-3828 ext. 284 or DSN 785-3828 ext. 284. Requests from non-U.S. Agencies must be forwarded to their country's Embassy in Washington, DC, Attention: Air Attache's Office.

Aircraft Combat Survivability Self Study Program

SURVIAC is pleased to announce the availability of the Aircraft Combat Survivability Self Study Program, SSSP. The SSSP has been funded by the Joint Aircraft Survivability Program (JASP) and was developed by Distinguished Professor Emeritus Dr. Robert E. Ball. Nearly all of the material in the program has been taken from the Prologue and Chapter 1 of the textbook "The Fundamentals of Aircraft Combat Survivability Analysis and Design, Second Edition," written by Dr. Ball and published by the American Institute of Aeronautics and Astronautics (AIAA) in late 2003.

The SSSP is available for free downloading from the SURVIAC website at: http://www.bahdayton.com/surviac/survivabilityeducation.htm.

You may also request a CD containing all four versions free of charge by using the inquiry form located at http://www.bahdayton.com/surviac/inquiry.aspx.

AUVSI Association for Unmanned Vehicle Systems International

NDIA National Defense Industrial Association — Strength Through Industry & Technology

JAS

Aircraft Survivability 2009

3-6 November 2009 • Naval Postgraduate School • Monterey, CA

This symposium will explore the robustness of current, planned and developing systems to survive the emerging threats from complex and adaptive adversaries, across the full range of military and civil operations through 2025.

Agenda to include:

- Evolving and Radical Threats - Irregular, Disruptive and Catastrophic
- Lessons Learned from the Battlefield and the Rest of the World
- Non-traditional Contributors to Survivability
- "Game-changing" Survivability concepts
- Resourcing Survivability Initiatives for Success
- Special Session: Crashworthiness Today and Tomorrow

Program Information:

Frank Swehosky, Program Chair	(817) 280-5758
Walter L. Whitesides, AUVSI	(703) 633-8483
Dennis Lindell, JASPO	(703) 604-1104

NDIA Administrative Information:

Meredith Geary, CMP, Associate Director	(703) 604-1104

Products Distributed by SURVIAC

The Survivability/Vulnerability Information Analysis Center (SURVIAC) is a U.S. Department of Defense Information Analysis Center (IAC) sponsored by the Defense Technical Information Center (DTIC)

Product	Cost
A Critical Review of Graphite Epoxy Laser Damage Studies	$ 50.00
A Summary of Aerospace Vehicle Computerized Geometric Descriptions for For Vulnerability Analyses	$100.00 (Free to Gov't)
Advanced Materials for Enhanced Survivability	$100.00
Aircraft Combat Survivability Self Study Program (SSSP) CD (or download from SURVIAC website)	Free
Aircraft Fuel System Fire and Explosion Suppression Design Guide	$150.00
"Aircraft Survivability" Video	$ 50.00
Alternatives for Halon 1301 in Ground Vehicle Firefighting Systems	$250.00
An Overview of Laser Technology and Applications	$ 50.00
An Overview of Laser-Induced Eye Effects	$150.00
"Battle Damage Repair of Composite Structures" Video	$ 75.00
Collection of Vulnerability Test Results for Typical Aircraft Systems and Components	$150.00
Comparative Close Air Support Vulnerability Assessment Study - Executive Summary	Free
Compendium of References for Nonnuclear Aircraft Survivability (A supplement to MIL-HDBK-336)	$150.00
Component Vulnerability Workshop Component Pd/h Handbook	$200.00 (Free to Gov't)
Component Vulnerability Analysis Archive (CVAA) and Workshop Notes	$300.00 (Free to Gov't)
Component Vulnerability Database Development	$100.00 (Free to Gov't)
Computerized Geometric Information to Support Vulnerability Assessments State-of-the-Art Report	$ 75.00
Continuity of Operations (COOP) State-of-the-Art Report (SOAR)	$ 50.00
Countermeasures Handbook for Aircraft Survivability	$200.00 (Free to Gov't)
Critical Review and Technology Assessment (CRTA) for Soldier Survivability (Ssv)	$ 50.00
"Designing for Survivability" Video	Free??
Directed Energy Effectiveness Modeling State-of-the-Art Report (SOAR)	$ 50.00
DREAM Sensitivity Study	$ 50.00
"Fundamentals of Ground Combat System Ballistic Vulnerability/Lethality" by Dr. Paul Deitz	Free - Gov't only*
Gas Explosion Suppression Agent Investigation	$200.00
Joint Aircraft Survivability Program (JASP) Promotional Video	Free
Joint Live Fire/Live Fire Test Program Catalogue	$ 95.00
Lessons Learned from Live Fire Testing	$ 50.00 (Free to Gov't)
MANPADS Threats to Aircraft: A Vulnerability Perspective, February 2000, Final Report	$200.00
Missile Warhead Bomb and Propellant Response State-of-the-Art Report (SOAR)	$ 50.00
MOSAIC Sensitivity Study	$ 50.00
Munition Response State-of-the-Art Report (SOAR)	$ 50.00
National MANPADS Workshop: A Vulnerability Perspective, Proceedings - 2 volumes	$200.00
Night Vision Goggle (NVG) Rocket Propelled Grenade (RPG) Quick Look Report (QLR) CD	$ 50.00 (Free to Gov't)
Penetration Characteristics for Advanced Engine Materials	$100.00
Proceedings of the Eighth DoD Conference on DEW Vulnerability, Survivability, and Effects - 2 Volumes	$125.00 / per set
RADGUNS 1.8 Parametric Study	$100.00 (Free to Gov't)
Ship Survivability Overview	$ 50.00
SOAR on Directed Energy Weapon (DEW) Assessment Methods	$ 50.00
State-of-the-Art (SOAR) for Non-Lethal Weapon (NLW) Assessment Methodologies	$ 50.00
"SURVIAC - A Capabilities Overview" Video	30-day loan
"The Fundamentals of Aircraft Combat Survivability Analysis and Design" second edition, by Robert E. Ball	Free - Gov't Only*
"Threat Effects in Aircraft Combat Survivability" Video (2006)	$ 50.00 (Free to Gov't)
Threat Warheads and Effects / Battle Damage Assessment and Repair Archival and Retrieval (TWE/BDAR) System	$300.00
Ullage Explosion Hazard State-of-the-Art Report (SOAR)	$ 50.00
U.S. Air Force Surface-to-Air Engagement During Operation Desert Storm	$100.00
Vulnerability Reduction Design Guide for Ground Systems in a Conventional Combat Environment	$200.00

* These books are free to U.S. Government employees through SURVIAC. All others may purchase these books through the American Institute of Aeronautics and Astronautics (AIAA), 800-639-2422, www.aiaa.org, or by e-mail at custserv@aiaa.org.

For further information on how to obtain these products and how to establish need-to-know certification, please contact SURVIAC at (937) 255-3828 ext. 284 or DSN 785-3828 ext. 284. Requests from non-U.S. Agencies must be forwarded to their country's Embassy in Washington, DC, Attention: Air Attache's Office.

Calendar of Events

SEPTEMBER 2009

2009 Homeland Security Symposium and Exhibition-"Building a Resilient & Sustainable Homeland - Public & Private Sector Partners Serving America"
9-10 Sep 2009
Crystal City, VA
POC: Mary Anna Christiansen, (703) 247-2596
e-mail: mchristiansen@ndia.org
www.ndia.org

NGAUS General Conference
11-13 Sep 2009
Nashville, TN
POC: NGAUS, (202) 789-0031
http://www.ngaus.org/content.asp?bid=8207

AIAA SPACE 2009 Conference & Exposition
14-17 Sep 2009
Pasadena, CA
POC: AIAA, (800) 639-2422
e-mail: custserv@aiaa.org

AOC 6th Multinational Passive Covert Radar Conference (PCR-2009)
15-17 Sep 2009
Verona, NY
POC: AOC, (703) 549-1600
www.crows.org

Global Deterrence and Defense Symposium 2009 - "National Security: Achieving Global Deterrence and Defense"
15-16 Sep 2009
Bloomington, IN
POC: Pamela Ingram, (812) 854-3239
e-mail: pamela.ingram@navy.mil

2009 SURVIAC Liaison Workshop
28 Sep - 30 Sep 2009
Wright-Patterson AFB, OH
POC: SURVIAC, Donna Egner, (937) 255-3828 x282
e-mail: egner_donna@bah.com

2009 Annual ITEA Symposium
28 Sep - 1 Oct 2009
Baltimore, MD
POC: ITEA, (703) 631-6220
http://www.itea.org/Annual_Symposium.asp

OCTOBER 2009

2009 Combat Vehicles Conference
12-14 Oct 2009
Dearborn, MI
POC: Suzanne Havelis, (703) 247-2561
e-mail: shavelis@ndia.org

2009 TACOM LCMC APBI-"Supporting the Warfighters for Present Conflicts and Future Missions"
14-16 Oct 2009
Dearborn, MI
POC: Holley Slabaugh , (703) 247-2561
e-mail: hslabaugh@ndia.org

MILCOM 2009-"The Challenge of Convergence"
18-21 Oct 2009
Boston, MA
POC: Jack Barry, (800) 564-4220
e-mail: jack.barry@milcom09.com
http://www.milcom.org/index.html

46th Annual AOC International Symposium and Convention-"Modernizing EW: Balancing Costs and Capability"
18-22 Oct 2009
Washington, DC
POC: AOC, (703) 549-1600
www.crows.org

47th Annual Targets, UAVs & Range Operations Symposium & Exhibition
21-23 Oct 2009
Savannah, GA
POC: Meredith Geary, (703)247-9476
e-mail: mgeary@ndia.org

19th Annual International Aircraft Fire Protection/ Mishap Investigation Course
26-30 Oct 2009
Dayton, OH
POC: Robert Clodfelter, (937) 435-8778
afp1fire@aol.com
http://www.afp1fire.com/

NOVEMBER 2009

Twelfth Annual Directed Energy Symposium
2-6 Nov 2009
San Antonio, TX
POC: Cynnamon Spain , (505) 998-4910
e-mail: cynnamon@deps.org
http://www.deps.org/DEPSpages/DEsymp09.html

2009 End to End Testing Workshop
2-5 Nov 2009
San Diego, CA
POC: ITEA, (703) 631-6220
http://itea.org/2009_End_to_End%20Testing.asp

NDIA Aircraft Survivability 2009: "Next Generation Requirements"
3-6 Nov 2009
Monterey, CA
POC: Meredith Geary, (703) 247-9476
e-mail: mgeary@ndia.org
http://www.ndia.org

Combatant Commanders Workshop
3-4 Nov 2009
Tampa, FL
POC: DTIC, (703) 767-8267
e-mail: DTICCoComWorkshop@dtic.mil
http://www.dtic.mil/dtic

National Homeland Defense Symposium VII
9-11 Nov 2009
Colorado Springs, CO
POC: NHDF, Eleanor Martinez, (719) 577-9016
e-mail: emartinez@nhdf.org
http://www.nhdf.com

USCG Innovation Expo
17-19 Nov 2009
Virginia Beach, VA
POC: Angie R. DeKleine, or (703) 247-2599
e-mail: adekleine@ndia.org

The Interservice/Industry Training, Simulation and Education Conference (I/ITSEC) - Train to Fight-Fight to Win
30 Nov-3 Dec 2009
Orlando, Fl
POC: Barbara McDaniel, (703) 247-2569
e-mail: bmcdaniel@ndia.org

Visit our website for more event listings and information: http://iac.dtic.mil/surviac

SURVIAC

780 TS/OL-AC/SURVIAC

2700 D Street., Building 1661

Wright-Patterson AFB, OH 45433-7404

Requests from non-U.S. Citizens/agencies must be forwarded to their country's embassy in Washington, D.C., Attn: Air Attache's Office.

SURVIAC Information Request (U.S. Citizens Only)

☐ Change the distribution information as show below.

☐ Subscribe me to the SURVIAC Bulletin.

○ Hard Copy ○ Electronic Copy (.pdf) ○ Both

☐ Subscribe me to the SURVIAC E-News, a weekly e-mail news update for the survivability/vulnerability/lethality community.

☐ Subscribe me to the SURVIAC Dynamic Events Calendar, a monthly e-mail calendar of events of interest to the survivability/vulnerability/lethality community.

☐ Subscribe me to the JASP Aircraft Survivability Journal.

○ Hard Copy ○ Electronic Copy (.pdf) ○ Both

Name: _____

(prefix, first, MI, last)

Company/Org: _____

Address: _____

_____

City/State/Zip: _____

Phone: _____

E-mail: _____

Service: ○ USAF ○ USN ○ USA ○ USMC ○ USCG ○ DoD ○ Other U.S. Gov't. Org ○ Contractor

☐ Request a SURVIAC Model Guide

○ Hard Copy ○ Electronic Copy (.pdf)

☐ Request SURVIAC Technical Area Task (TAT) Information (Government only)

☐ Request SURVIAC Subscription Information (Government and Contractors only)

Please visit our website to subscribe to our newsletters or request information via the inquiry form on our website: *http://iac.dtic.mil/surviac*.

If you prefer, mail this form to:
SURVIAC Subscriptions
780 TS/OL-AC/SURVIAC
2700 D Street, Building 1661
Wright-Patterson AFB, OH 45433-7404

or Fax to (937) 255-9673

For immediate assistance please call us:
(937) 255-3828, DSN: 785-3828